



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,758	12/12/2003	Taro Ishikawa	010755.52992US	8747
23911 7590 07/29/2010 CROWELL & MORING LLP INTELLECTUAL PROPERTY GROUP P.O. BOX 14300 WASHINGTON, DC 20044-4300				
EXAMINER KAO, RUTAI				
ART UNIT 2473		PAPER NUMBER		
MAIL DATE 07/20/2010		DELIVERY MODE PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/733,758

Applicant(s)

ISHIKAWA ET AL.

Examiner

JUTAI KAO

Art Unit

2473

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 May 2010.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 4-6 and 9 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 4-6 and 9 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/22)
- Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/17/2010 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 6 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claim 6, the applicant further argues that Bass does not teach the feature of the packet filter/analysis portion are "related to the internal operations of the automatic detecting apparatus, and thus are not directed to the network operation" as Bass discloses a LAN switch that performs the analyzing of the header. However, the claimed portion that Bass was relied on to reject only requires a packet receiving portion used to receive communication and determine whether data retention is necessary (as shown by the I/O logic and cut through/store and forward decision logic in Fig. 3 of Bass) and the packet filter/analysis portion that analyzes the header information (which is shown in column 2, lines 52-56, which recites a LAN switch that analyzes the header

information in order to perform the forwarding of the packet using the cut-through mode of operation; therefore, it is clear that the device shown in Fig. 3 of Bass is the improved LAN switch, which allows both cut-through and store-and-forward). Therefore, Bass does include a single device that includes the claimed packet receiving portion and the packet filter/analysis portions.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 1 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klinker (US 2007/0140128) in view of Bass (US 6,144,668).

Klinker discloses a system and method to provide routing control of information over networks including the following features.

Regarding claim 1, an automatic detecting method for detecting protocol nonconformity in TCP/IP (see "Flow control system 90 further operates to detect when one or more rules, or flow policies, are violated..." recited in paragraph [0061]; where the violation of policy represents a nonconformity of the protocol, and the flow control process being the transmission/reception control process; also see "TCP" recited in paragraph [0008] and "IP" recited in paragraph [0050]), occurring in the communications between transmitting and receiving terminals (see user terminals shown in Fig. 1C) that make at least one transmitting and receiving control process in accordance with TCP/IP (see "TCP" recited in paragraph [0008] and "IP" recited in paragraph [0050]), in a case where at least one of: a communication apparatus does not perform its operation in accordance with the specifications of the TCP/IP (see "flow control system 90 enforces policies associated with data traffic flow by correcting detrimental deviations in performance..." recited in paragraph [0061]; such that the transmitting/receiving devices are not operating in accordance with its traffic contract as set forth in its TCP/IP communication); an expected communication process is not performed in the TCP/IP due to false mounting; and an expected communication process does not operate in a new application because of a deficiency or defect in the TCP/IP, said method comprising: receiving a packet transmitted or received in the communication between said transmitting and receiving terminals (see "packet capture 650" in Fig. 6 and "receive captured raw packets" recited in paragraph [0105]);

analyzing header information of the packet transferred from the receiving (see "parser 651 extracts information from the IP and TCP headers" recited in paragraph [0105], and see passive flow analyzer 330/630, which analyzes the received flow in Fig. 3 and 6);

creating state information, which is TCP connection information (see "TCP flow" recited in paragraph [0008], that TCP flows are used in the system, thus the flow policies are considered TCP connection information policies) regarding a state of transmitting or receiving the packet (see "Traffic flows are monitored within passive calibrator 203 according to the underlying protocol state" recited in paragraph [0083], and see "Packet loss is calculated...by maintaining the state of all of the retransmitted packets that occur" recited in paragraph [0112], the two passages both show the calculation of state information regarding the packet flows) to correspond to a result of transmitting and receiving control in accordance with said communication protocol (see "DSCP information encoded in the ToS (i.e., "type of service") bits...information about IP packet QoS requirements...Per Hop Behavior of a traffic class..." recited in paragraph [0105], that is, information regarding the protocol, or policy, is extracted based on the header information (see "extracts information from the...headers" recited in paragraph [0105]) and the payload information transferred from the analyzing (see "inspect the payload of each packet...to interpret the performance and operation..." recited in paragraph [0103]) of a required kind of the packet, in an actual communication state (see "Flow control system 90 makes such corrections based on real- or near-real time traffic analysis" recited in paragraph [0061]);

estimating normal information of a case where the transmitting and receiving control process is normally performed (see policy repository 218 in Fig. 2, which holds the normal ranges of parameters acceptable to the policy corresponding to the packet streams) with the header information and the payload information received from the creating (see "rules, or flow policies" recited in paragraph [0061] or see extracts information from the IP and TCP headers. Such extracted information...includes...DSCP information...about IP packet QoS requirement..." recited in paragraph [0105]);

storing beforehand nonconformity information featuring nonconformity in the transmitting and receiving control process (see policy repository 218 in Fig. 2 and see "policy repository 218...typically include service level agreement (SLA) performance metrics" recited in paragraph [0135]) the nonconformity information being any one of a conditional formula regarding the TCP connection information, a conditional formula regarding the header information of the packet, and a combination thereof (see "determine if a flow policy is violated" recited in paragraph [0064], which shows a conditional formula is used, wherein as shown above and see "TCP flow" recited in paragraph [0008], that TCP flows are used in the system, thus the flow policies are considered TCP connection information policies); and

comparing the analysis result of the analyzing, the TCP connection information created by the creating (see "The aggregated flow data 680 is communicated to controller 605 and is used by the controller to determine whether the current traffic flow violates or fails to conform to an associated flow policy for a given destination" as

recited in paragraph [0101]; wherein the aggregated flow data and the flow characteristics used in the determining, as shown in step 6, is a result of analyzing the header information and the flow characteristic is the created state information regarding the flow, as performed by parser 651 and correlator 652), the normal information estimated by the estimating (see rejection above regarding the estimating step, in which "rules, or flow policies" recited in paragraph [0061] or see "extracts information from the IP and TCP headers. Such extracted information...includes...DSCP information...about IP packet QoS requirement..." recited in paragraph [0105], wherein the normal information is estimated by the predefined flow policies), and the nonconformity information stored by the storing (see "If a particular policy is violated (i.e., one or more performance metrics are outside one or more expected ranges or values)..." recited in paragraph [0135]) to detect the transmitting and receiving control process where said nonconformity has occurred (see "detect when one or more rules, or flow policies, are violated" recited in paragraph [0061] or the detection of violation condition shown in paragraph [0135], in both cases the nonconformity, or the violation of policy, is detected for the transmitting and receiving control process, or the flow control process).

Regarding claim 6, an automatic detecting apparatus for detecting protocol nonconformity in TCP/IP occurring in a communication between transmitting and receiving terminals (see "Flow control system 90 further operates to detect when one or more rules, or flow policies, are violated..." recited in paragraph [0061]; where the violation of policy represents a nonconformity of the protocol, and the flow control process being the transmission/reception control process), occurring in the

communications between transmitting and receiving terminals (see user terminals shown in Fig. 1C) that make at least one transmitting and receiving control process in accordance with TCP/IP (see "TCP" recited in paragraph [0008] and "IP" recited in paragraph [0050]), said method comprising:

- a packet receiving portion that receives a packet transmitted or received in the communication between said transmitting and receiving terminals (see "packet capture 650" in Fig. 6 and "receive captured raw packets" recited in paragraph [0105]);

- a packet filter/analysis portion that analyzed header information of the packet transferred from the receiving (see "parser 651 extracts information from the IP and TCP headers" recited in paragraph [0105], and see passive flow analyzer 330/630, which analyzes the received flow in Fig. 3 and 6);

- a connection information calculating portion that creates state information, which is TCP connection information (see "TCP flow" recited in paragraph [0008], that TCP flows are used in the system, thus the flow policies are considered TCP connection information policies) regarding a state of transmitting or receiving the packet (see "Traffic flows are monitored within passive calibrator 203 according to the underlying protocol state" recited in paragraph [0083], and see "Packet loss is calculated...by maintaining the state of all of the retransmitted packets that occur" recited in paragraph [0112], the two passages both show the calculation of state information regarding the packet flows) to correspond to a result of transmitting and receiving control in accordance with said communication protocol (see "DSCP information encoded in the ToS (i.e., "type of service") bits...information about IP packet QoS requirements...Per

Hop Behavior of a traffic class..." recited in paragraph [0105], that is, information regarding the protocol, or policy, is extracted) based on the header information (see "extracts information from the...headers" recited in paragraph [0105]) and the payload information transferred from the analyzing (see "inspect the payload of each packet...to interpret the performance and operation..." recited in paragraph [0103]) of a required kind of the packet, in an actual communication state (see "Flow control system 90 makes such corrections based on real- or near-real time traffic analysis" recited in paragraph [0061]);

a normal information estimating portion that estimates normal information of a case where the transmitting and receiving control process is normally performed (see policy repository 218 in Fig. 2, which holds the normal ranges of parameters acceptable to the policy corresponding to the packet streams) with the header information and the payload information received from the creating (see "rules, or flow policies" recited in paragraph [0061] or see extracts information from the IP and TCP headers. Such extracted information...includes...DSCP information...about IP packet QoS requirement..." recited in paragraph [0105]);

a nonconformity information saying portion that stores beforehand nonconformity information featuring nonconformity in the transmitting and receiving control process (see policy repository 218 in Fig. 2 and see "policy repository 218...typically include service level agreement (SLA) performance metrics" recited in paragraph [0135]) the nonconformity information being any one of a conditional formula regarding the TCP connection information, a conditional formula regarding the header information of the

packet, and a combination thereof (see "determine if a flow policy is violated" recited in paragraph [0064], which shows a conditional formula is used, wherein as shown above and see "TCP flow" recited in paragraph [0008], that TCP flows are used in the system, thus the flow policies are considered TCP connection information policies); and

a nonconformity comparison determining portion that compares the analysis result of the analyzing, the TCP connection information created by the creating (see "The aggregated flow data 680 is communicated to controller 605 and is used by the controller to determine whether the current traffic flow violates or fails to conform to an associated flow policy for a given destination" as recited in paragraph [0101]; wherein the aggregated flow data and the flow characteristics used in the determining, as shown in step 6, is a result of analyzing the header information and the flow characteristic is the created state information regarding the flow, as performed by parser 651 and correlator 652), the normal information estimated by the estimating (see rejection above regarding the estimating step, in which "rules, or flow policies" recited in paragraph [0061] or see "extracts information from the IP and TCP headers. Such extracted information...includes...DSCP information...about IP packet QoS requirement..." recited in paragraph [0105], wherein the normal information is estimated by the predefined flow policies), and the nonconformity information stored by the storing (see "If a particular policy is violated (i.e., one or more performance metrics are outside one or more expected ranges or values)..." recited in paragraph [0135]) to detect the transmitting and receiving control process where said nonconformity has occurred (see "detect when one or more rules, or flow policies, are violated" recited in paragraph

[0061] or the detection of violation condition shown in paragraph [0135], in both cases the nonconformity, or the violation of policy, is detected for the transmitting and receiving control process, or the flow control process).

Klinker does not disclose the following features: regarding claims 1 and 6, receiving at a network interface a packet to transfer the packet for data retention if it is necessary to save the packet, and to transfer the packet for packet analysis, unless it is necessary to save the packet; and wherein the analyzing is performed in order to transfer the header information and necessary payload information.

Bass discloses a system including simultaneous cut through and store-and-forward frame support including the following features.

Regarding claims 1 and 6, receiving at a network interface (see Receive Frame I/O logic 302 in Fig. 3) a packet to transfer the packet for data retention if it is necessary to save the packet, and to transfer the packet for packet analysis, unless it is necessary to save the packet (see system shown in Fig. 3, in which the cut through/store and forward decision logic 306 determines whether to transmit a received packet from using store and forward or cut through; in which, if it is determined that store and forward needs to be performed, then saving the packet is necessary and the packet is stored for data retention prior to being forwarded; if it is determined that the packet is to be transmitted using cut through, then "the LAN switch analyzes the address information contained in a frame header, and immediately begins transferring data received from one LAN segment to the destination LAN segment as determined by the address information" recited in column 2, lines 52-56; that is, data is transferred for analyzes and

forwarding when store-and-forward is not required and the cut-through mode is selected); and

analyzing header information of the packet transferred from the receiving portion to transfer the header information and necessary payload information (see "analyzes the address information contained in a frame header, and immediately begins transferring data received from one LAN segment to the destination LAN segment as determined by the address information" recited in column 2, lines 52-56).

It would have been obvious to one of the ordinary skill in the art at the time of the invention to modify the system of Klinker using features, as taught by Bass, in order to enable "simultaneous cut-through and store-and-forward transmission of frames in high speed network devices" as recited in the abstract of Bass.

4. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Klinker and Bass as applied to claim 1 above, and further in view of Hernandez-Valencia (US 6,266,327).

Klinker and Bass disclose the claimed limitations as shown above.

Klinker and Bass do not disclose the following features: regarding claim 4, wherein said calculation step further comprises updating said state information every time acquiring the packet, and said comparison further comprises comparing the latest state information updated at said calculation step and said nonconformity information.

Hernandez-Valencia discloses a non-conformance indicator for the guaranteed frame rate service including the following features.

Regarding claim 4, wherein said calculation step further comprises updating said state information every time acquiring the packet (see “a new cell from the received data stream arrives...” recited in column 6 line 11-29 and Fig. 3-8; where each of the conformance check algorithm flowcharts in Fig. 3-8 shows a series of checks performed on each new cell received and updating values, such as Cnt in step 325, 425, etc.), and said comparison step further comprises comparing the latest state information updated at said calculation step and said nonconformity information (see Fig. 3, step 330, checking the calculated Cnt against the MFS).

It would have been obvious to modify the system of Klinker and Bass using features, as taught by Hernandez-Valencia, in order to conduct nonconformance test of received packet size.

5. Claims 5 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Klinker and Bass as applied to claims 1 and 6 above, and further in view of Aoki (US 6,757,255).

Klinker and Bass disclose the claimed limitations as shown above.

Klinker and Bass do not disclose the following features: regarding claims 5 and 9, wherein the TCP connection information includes an evaluation value having at least one of a total number of transmitted packets, a total number of retransmitted packets, a total number of Selective ACKnowledgement (SACK) blocks, a minimum packet size, a throughput of a maximum retransmitted interval, and a round trip time up to receiving a response packet to the transmitted packet.

Aoki discloses an apparatus for and method of measuring communication performance including the following features.

Regarding claims 5 and 9, wherein the TCP connection information (explained in the rejection made to claim 1) includes an evaluation value having at least one of a total number of transmitted packets (see "total number of packets" recited in claim 6), a total number of retransmitted packets (see "the number of packets re-transmitted" recited in claim 6), a total number of Selective ACKnowledgement (SACK) blocks, a minimum packet size (see "minimum value of MTU..." recited in column 11, lines 45), a throughput of a maximum retransmitted interval, and the round trip time (see "round trip time" recited in column 7, line 26) up to receiving a response packet (see "an ACK packet receiving time" recited in column 3, line 32) to the transmitted packet (see SYN packet transmitting time" recited in column 3, line 31-32) .

It would have been obvious for one of the ordinary skill in the art at the time of the invention to modify the system of Klinker and Bass by using the features, as taught by Aoki, in order to better detect nonconformance of data transmission.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUTAI KAO whose telephone number is (571)272-9719. The examiner can normally be reached on Monday ~Friday 7:30 AM ~5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang Yao can be reached on (571)272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ju-Tai Kao
/Ju-Tai Kao/
Acting Examiner of Art Unit 2473

/KWANG B. YAO/
Supervisory Patent Examiner, Art Unit 2473